PAYMENT DATA SECURITY ESSENTIAL

Patching

WHAT'S THE RISK?

80% of hacking attacks could be prevented by strengthening passwords and **installing software patches**

(2017 Verizon Data Breach Investigation Report)

Unpatched software is one of the leading causes of data breaches for businesses.

Often, software has flaws or mistakes made by programmers when they wrote the code. Vendors regularly issue updates known as patches to fix these software vulnerabilities. When businesses don't apply software patches from vendors hackers exploit these vulnerabilities to break into their computers and systems and steal payment data.

PATCHING BEST PRACTICES

Timely installation of security patches is crucial to minimize the risk of being breached. In order to apply patches quickly, it is important that you know how your software is being regularly updated with patches and who is responsible (it could be you!).

Identify which vendors send you patches

The Questions to Ask Your Vendors resource can help businesses identify which vendors send you patches. These include vendors of your payment terminal, payment applications, other payment systems (tills, cash registers, PCs, etc.), operating systems (Android, Windows, iOS, etc.), application software (including your web browser), and business software.

Talk to your vendors about patches

Make sure your vendors update your payment terminals, operating systems, etc. so they can support the latest security patches. Ask them how patches get added (some install automatically when they become available) and who is responsible. Find out how they notify you of new security patches, and make sure you receive and read these notices.

Install patches

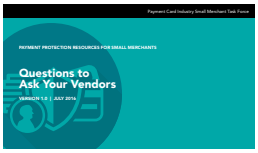
Follow your vendors' instructions and install patches as soon as possible.

Don't ignore e-commerce

E-commerce businesses should look out for patches from your payment service provider. Ask your e-commerce hosting provider whether they patch your system (and how often). Make sure they update the operating system, e-commerce platform and/or web application so it can support the latest patches.

RESOURCES

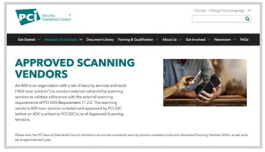
Visit **pcissc.org/Merchants** for more resources



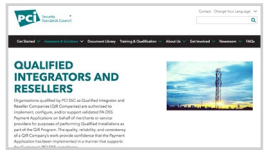
The Questions to Ask Your Vendors resource can help businesses identify which vendors send you patches.

The Guide to Safe Payments provides businesses with security basics to protect against payment data theft.

Watch this quick animated video to learn how businesses can minimize the chances of being breached by installing software patches quickly.



Vulnerability scanning tools provided by PCI Approved Scanning Vendors can also help businesses automatically search your networks to find vulnerabilities and report when patches need to be applied.



The PCI Qualified Integrators and Resellers (QIR) list is a resource businesses can use to find payment system installers that have been trained by the PCI Security Standards Council on patching and other payment data security essentials.

PCI Security Standards Council